

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Brian Jacoby et al.	Art Unit	: 2143
Serial No.	: 09/894,918	Examiner	: Alina Boutah
Filed	: June 29, 2001	Conf. No.	: 5947
Title	: DEEP PACKET SCAN HACKER IDENTIFICATION		

**Mail Stop Appeal Brief - Patents**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

BRIEF ON APPEAL

**(1) Real Party in Interest**

America Online LLC. is the real party in interest.

**(2) Related Appeals and Interferences**

There are no related appeals or interferences

**(3) Status of Claims**

Claims 1, 3-7, 11-12, 16-17, 19-20, 22-26, 28, 30-31, 35-36, 38-39, 41-45, 47, 49-50, 54-55, 57-62, 64 and 67-73 are pending, with claims 1, 20, and 39 being independent.

**(4) Status of Amendments**

All amendments have been entered.

**(5) Summary of Claimed Subject Matter**

Independent claim 1 is directed to a method for securing an accessible computer system. See, e.g., Application, Page 14, Line 30 to page 18, Line 23; Fig. 6 and Fig. 7.

The method includes receiving more than one data packet at a network device, each data packet including a payload portion and an attribute portion and being communicated between at least one access requestor and at least one access provider through the network device. See, e.g., Application, Page 15, Line 20 to page 16, Line 6; Fig. 6 and Fig. 7.

The method also includes monitoring, at the network device, at least the payload portion of the data packets directed from at least one of the access providers to at least one of the access

requestors by scanning the payload portion for at least one predetermined pattern and counting a number of data packets having payload portions that include the predetermined pattern. See, e.g., Application, Page 17, Line 1 to page 17, Line 20; Fig. 6 and Fig. 7.

The method also includes using the network device to deny communication of subsequent data packets from the access requestor to the access provider when a number of payload portions of the data packets received from the access provider to the access requestor are deemed to include the predetermined pattern exceed a configurable threshold number. See, e.g., Application, Page 17, Line 12 to page 17, Line 20; Fig. 6 and Fig. 7.

Independent claim 20 is directed to a system that connects a plurality of access requestors to a plurality of access providers for securing an accessible computer system. See, e.g., Application, Page 14, Line 30 to page 18, Line 23; Fig. 3, Fig. 6 and Fig. 7.

The system includes a receiving component that is structured and arranged to receive more than one data packet, each data packet including a payload portion and an attribute portion and being communicated between at least one access requestor and at least one access provider. See, e.g., Application, Page 15, Line 20 to page 16, Line 6; Fig 3, Fig. 6 and Fig. 7.

The system also includes a monitoring component that is structured and arranged to monitor at least the payload portion of the data packets directed from at least one of the access providers to at least one of the access requestors and includes a scanning component that is structured and arranged to scan the payload portion for at least one predetermined pattern and to count a number of data packets having payload portions that include the predetermined pattern. See, e.g., Application, Page 17, Line 1 to page 17, Line 20; Fig. 3, Fig. 6 and Fig. 7.

The system also includes an access controlling component that is structured and arranged to deny communication of subsequent data packets from the access requestor to the access provider when a number of payload portions of data packets received from the access provider to the access requestor that include the predetermined pattern exceed a configurable threshold number. See, e.g., Application, Page 17, Line 12 to page 17, Line 20; Fig. 3, Fig. 6 and Fig. 7.

Independent claim 39 is directed to a computer program stored on a network device computer that connects a plurality of access requestors to a plurality of access providers for securing an accessible computer system. See, e.g., Application, Page 14, Line 30 to page 18, Line 23; Fig. 3, Fig. 6 and Fig. 7.

The computer program includes a receiving code segment that causes the computer to receive more than one data packet, each data packet including a payload portion and an attribute portion and being communicated between at least one access requestor and at least one access provider. See, e.g., Application, Page 15, Line 20 to page 16, Line 6; Fig 3, Fig. 6 and Fig. 7.

The computer program also includes a monitoring code segment that causes the computer to monitor at least the payload portion of the data packets directed from at least one of the access providers to at least one of the access requestors and includes a scanning code segment that causes the computer to scan the payload portion for at least one predetermined pattern and to count a number of data packets having payload portions that include the predetermined pattern. See, e.g., Application, Page 17, Line 1 to page 17, Line 20; Fig. 3, Fig. 6 and Fig. 7.

The computer program also includes an access controlling code segment that causes the computer to deny subsequent communication of data packets from the access requestor to the access provider when a number of payload portions of the data packets received from the access provider to the access requestor that include the predetermined pattern exceed a configurable threshold number. See, e.g., Application, Page 17, Line 12 to page 17, Line 20; Fig. 3, Fig. 6 and Fig. 7.

#### **(6) Grounds of Rejection to be Reviewed on Appeal**

Claims 1, 3-7, 11-12, 16-17, 19-20, 22-26, 28, 30-31, 38-39, 41-45, 47, 49-50, 54-55, 57-62, 64 and 68-73 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Cox (U.S. 6,738,814) in view of Eichstaedt et al. (U.S. 6,662,230) and in further view of Maher, III et al. (U. S. 6,654,373), in further view of Alcendor (U. S. 6,337,899).

#### **(7) Argument**

**The Rejection Of Claims 1, 3-7, 11-12, 16-17, 19-20, 22-26, 28, 30-31, 38-39, 41-45, 47, 49-50, 54-55, 57-62, 64 and 68-73 as being unpatentable over Cox (U.S. 6,738,814) in view of Eichstaedt et al. (U.S. 6,662,230) and in further view of Maher, III et al. (U. S. 6,654,373), in further view of Alcendor (U. S. 6,337,899) Should Be Reversed.**

1. The combination of Cox, Eichstaedt, Maher, and Alcendor fails to disclose at least one feature recited by those claims – namely “monitoring, at the network device, at least the payload



portion of the data packets directed from at least one of the access providers to at least one of the access requestors by scanning the payload portion for at least one predetermined pattern and counting a number of data packets having payload portions that include the predetermined pattern; and using the network device to deny subsequent data packets from the access requestor to the access provider when a number of payload portions of the data packets received from the access provider to the access requestor is deemed to include the predetermined pattern exceed a configurable threshold number”, as recited in claim 1 and similarly recited in claims 20, and 39.

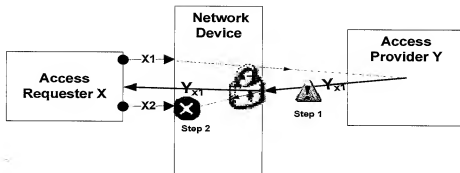
In independent claim 1, Applicant claims a method that includes, *inter alia*, monitoring, at the network device, at least the payload portion of the data packets directed from at least one of the access providers to at least one of the access requestors by scanning the payload portion for at least one predetermined pattern and counting a number of data packets having payload portions that include the predetermined pattern; and using the network device to deny subsequent data packets from the access requestor to the access provider when a number of payload portions of the data packets received from the access provider to the access requestor is deemed to include the predetermined pattern exceed a configurable threshold number.

Applicant respectfully requests reconsideration and withdrawal of the rejection because not any one of the four references, Cox, Eichstaedt, Maher and Alcendor, nor any possible combination of these references, discloses or suggests the feature of denying subsequent data packets from access requestors based on the results of monitoring the payload portion of the data packets directed from access providers, as claimed.

On the record, Applicant has illustrated that all four references fail to teach the feature above. However, the advisory action provides no new arguments in response to Applicant's illustration and merely relies on the “combination as cited in the previous rejection”.

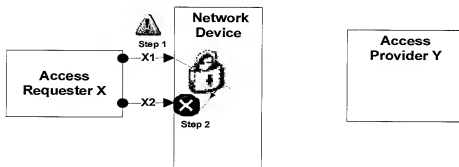
Applicant further illustrates an aspect of this feature recited by claim 1 using FIG. 1. below:

- Step 1:  The Network Device monitors  $Y_{x1}$ , a data packet from the Access Provider Y to Access Requester X to determine whether it has a predetermined pattern.
- Step 2:  The Network Device denies  $X2$ , a data packet from the same Access Requester X if the number of data packets  $Y_{x1}$  from Access Provider Y to Access Requester X having the predetermined pattern exceeds a threshold.



**FIG. 1 Claimed method**

Cox fails to teach step 1 of FIG. 1 above. In fact, Cox never monitors data packets from Access Provider Y. In contrast, Cox monitors solely data packets from the Access Requestor X. More specifically, as shown in FIG. 2 below, Cox denial of service decision is based solely on data packets from the incoming packets X1, X2 from the Access Requestor X.

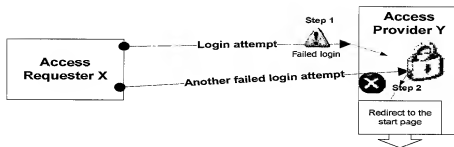


**FIG. 2 Cox's method**

The Office Action of 08/09/06 also acknowledges that Cox fails to suggest the features cited above. "Cox also fails to explicitly teach monitoring the payload portion of the data packets directed from at least one of the access providers to at least one of the access requestors..." See., e.g. page 5 of the Office Action of 08/09/06.

The Office Action of 08/09/06 similarly fails to rely on either of Eichstaedt or Maher for this feature, instead relying exclusively on Alcendor for the teaching of this feature. However,

Alcendor also fails to teach this feature.



**FIG. 3 Alcendor's method**

More specifically, Alcendor merely describes a method of authenticating users in telephony response systems, where users are temporarily inconvenienced to reselect the desired service after a number of failed login attempts, *see*, e.g., paragraph 2-3 of column 7 and Fig. 4 of Alcendor, also shown in FIG. 3 above, Alcendor only monitors the number of failed login attempts of a user; Alcendor does not monitor data packets from the access providers.

Additionally, in the response to the non-final Office action of 02/03/06, Applicant further clarified the distinction from Alcendor by pointing out that Alcendor lacks the use of an intermediary network device, as required by claim 1. By way of example, Alcendor does not disclose anything that relates to data packets, much less on monitoring the data packets directed from the access providers. Such additional distinction further demonstrates that Alcendor's system has a different structure and solves a different problem. This deficiency alone makes Alcendor unable to cure Cox's deficiency.

Therefore, the proposed combination of Alcendor, Cox, Eichstaedt and Maher is deficient for failure of any of these references to teach or suggest the feature of denying subsequent data packets from access requestors based on the results of monitoring the payload portion of the data packets directed from access providers, as claimed in independent claim 1, and similarly independent claims 20 and 39.

## 2. The Examiner's reasoning is based on improper hindsight reconstruction.

The Office Action and Advisory Action fail to make a *prima facie* case of obviousness capable of withstanding scrutiny, as each fails to set forth motivation for a combination of Alcendor and Cox.

The Examiner points out that reconstruction is proper so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made. Applicant does not dispute this point. However, Applicant nevertheless finds the reconstruction used by the Examiner to be improper, or at least without a proper basis.

The cited rules of law itself clearly specify the need for reconstruction to take account of only knowledge which was within the level of one of ordinary skill at the time of the invention. To establish a *prima facie* case of obviousness, the Examiner must therefore demonstrate that the level of knowledge available to those of ordinary skill at the time of the invention supports his hindsight reconstruction. The Examiner has not done so.

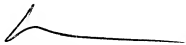
As indicated above, none of the art of record suggest the feature of denying subsequent data packets from access requestors based on the results of monitoring the payload portion of the data packets directed from access providers, and the Examiner has not demonstrated that those of ordinary skill at the time of the invention would have had knowledge of this very feature.

In view of the above, all of the claims should be in condition for allowance A formal notice of allowance is thus respectfully requested.

The fee in the amount of \$500 for the brief is being paid concurrently herewith on the Electronic Filing System (EFS) by way of Deposit Account authorization. Please apply any other charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: 5/2/2002

  
\_\_\_\_\_  
W. Karl Renner  
Reg. No. 41,265

Fish & Richardson P.C.  
1425 K Street, N.W.  
11th Floor  
Washington, DC 20005-3500  
Telephone: (202) 783-5070  
Facsimile: (202) 783-2331

### **Appendix of Claims**

1. (Previously presented) A method for securing an accessible computer system, the method comprising:

receiving more than one data packet at a network device, each data packet including a payload portion and an attribute portion and being communicated between at least one access requestor and at least one access provider through the network device;

monitoring, at the network device, at least the payload portion of the data packets directed from at least one of the access providers to at least one of the access requestors by scanning the payload portion for at least one predetermined pattern and counting a number of data packets having payload portions that include the predetermined pattern; and

using the network device to deny communication of subsequent data packets from the access requestor to the access provider when a number of payload portions of the data packets received from the access provider to the access requestor are deemed to include the predetermined pattern exceed a configurable threshold number.

2. (Canceled).

3. (Previously presented) The method as in claim 1 wherein monitoring the data packets includes scanning the payload portion while handling the data packets with a network device.

4. (Previously presented) The method as in claim 3 wherein monitoring the data packet includes monitoring only at least one data packet that is distinguished.

5. (Previously presented) The method as in claim 1 wherein:  
securing the accessible computer system further comprises distinguishing at least one of the data packets from among the data packets received for additional processing, and  
monitoring the payload portion includes monitoring the payload portion of the at least one data packet distinguished.

6. (Original) The method as in claim 5 wherein the at least one data packet is distinguished based on an Internet address associated with the data packet.

7. (Previously presented) The method as in claim 1 wherein monitoring the data packet includes monitoring all of the data packets received.

8-10. (Canceled).

11. (Previously presented) The method as in claim 1 wherein the predetermined pattern includes a login failure message communicated from the access provider to the access requestor.

12. (Previously presented) The method as in claim 1 wherein the data packets include a token-based protocol packet, or a TCP packet or a PPP packet.

13-15. (Canceled).

16. (Previously presented) The method as in claim 1 wherein denying communication of subsequent data packets includes affecting bandwidth for communications between the access requestor and the access provider.

17. (Previously presented) The method as in claim 1 further comprising rerouting the access requestor.

18. (Canceled).

19. (Previously presented) The method as in claim 1 wherein denying data packets from the access requestor to the access provider includes denying data packets from the access requestor to the access provider when a number of payload portions that include the predetermined pattern exceed a configurable threshold number during a configurable period of time.

20. (Previously presented) A system that connects a plurality of access requestors to a plurality of access providers for securing an accessible computer system, comprising:

a receiving component that is structured and arranged to receive more than one data packet, each data packet including a payload portion and an attribute portion and being communicated between at least one access requestor and at least one access provider;

a monitoring component that is structured and arranged to monitor at least the payload portion of the data packets directed from at least one of the access providers to at least one of the access requestors and includes a scanning component that is structured and arranged to scan the payload portion for at least one predetermined pattern and to count a number of data packets having payload portions that include the predetermined pattern; and

an access controlling component that is structured and arranged to deny communication of subsequent data packets from the access requestor to the access provider when a number of payload portions of data packets received from the access provider to the access requestor that include the predetermined pattern exceed a configurable threshold number.

21. (Canceled).

22. (Previously presented) The system of claim 20 wherein the monitoring component includes a scanning component that is structured and arranged to scan the payload portion while handling the data packets with a network device.

23. (Previously presented) The system of claim 22 wherein the monitoring component is structured and arranged to monitor only at least one data packet that is distinguished.

24. (Previously presented) The system of claim 20 wherein the system further comprises a distinguishing component that is structured and arranged to distinguish at least one of the data packets from among the data packets received for additional processing, and

the monitoring component is structured and arranged to monitor the payload portion of the at least one data packet distinguished.

25. (Original) The system of claim 24 wherein the at least one data packet is distinguished based on an Internet address associated with the data packet.

26. (Previously presented) The system of claim 20 wherein the monitoring component is structured and arranged to monitor all of the data packets received.

27. (Canceled).

28. (Previously presented) The system of claim 20 wherein the data packets are monitored when communicated from the access requestor to the access provider.

29. (Canceled).

30. (Previously presented) The system of claim 20 wherein the predetermined pattern includes a login failure message communicated from the access provider to the access requestor.

31. (Previously presented) The system of claim 20 wherein the data packets include a token-based protocol packet, or a TCP packet or a PPP packet.

32-34. (Canceled).

35. (Original) The system of claim 20 wherein the access controlling component is structured and arranged to affect bandwidth for communications between the access requestor and the access provider.

36. (Original) The system of claim 20 wherein the access controlling component is structured and arranged to reroute the access requestor.

37. (Canceled).

38. (Previously presented) The system of claim 20 wherein the access controlling component is structured and arranged to deny subsequent access by the access requestor to the access provider when a number of payload portions that include the predetermined pattern exceed a configurable threshold number during a configurable period of time.

39. (Previously presented) A computer program stored on a network device computer that connects a plurality of access requestors to a plurality of access providers for securing an accessible computer system, comprising:

a receiving code segment that causes the computer to receive more than one data packet, each data packet including a payload portion and an attribute portion and being communicated between at least one access requestor and at least one access provider;

a monitoring code segment that causes the computer to monitor at least the payload portion of the data packets directed from at least one of the access providers to at least one of the access requestors and includes a scanning code segment that causes the computer to scan the payload portion for at least one predetermined pattern and to count a number of data packets having payload portions that include the predetermined pattern; and

an access controlling code segment that causes the computer to deny subsequent communication of data packets from the access requestor to the access provider when a number of payload portions of the data packets received from the access provider to the access requestor that include the predetermined pattern exceed a configurable threshold number.

40. (Canceled).

41. (Previously presented) The computer program of claim 39 wherein the monitoring code segment includes a scanning code segment that causes the computer to scan the payload portion while handling the data packets with a network device.

42. (Previously presented) The computer program of claim 41 wherein the monitoring code segment causes the computer to monitor only at least one data packet that is distinguished.

43. (Previously presented) The computer program of claim 39 wherein:  
the computer program further comprises a distinguishing code segment that causes the computer to distinguish at least one of the data packets from among the data packets received for additional processing, and  
the monitoring code segment causes the computer to monitor the payload portion of the at least one data packet distinguished.

44. (Original) The computer program of claim 43 wherein the at least one data packet is distinguished based on an Internet address associated with the data packet.

45. (Previously presented) The computer program of claim 39 wherein  
the monitoring code segment causes the computer to monitor all of the data packets received.

46. (Canceled).

47. (Previously presented) The computer program of claim 39 wherein the data packets are monitored when communicated from the access requestor to the access provider.

48. (Canceled).

49. (Previously presented) The computer program of claim 39 wherein the predetermined pattern includes a login failure message communicated from the access provider to the access requestor.

50. (Previously presented) The computer program of claim 39 wherein the data packets include a token-based protocol packet, or a TCP packet or a PPP packet.

51-53. (Canceled).

54. (Original) The computer program of claim 39 wherein the access controlling code segment causes the computer to affect bandwidth for communications between the access requestor and the access provider.

55. (Original) The computer program of claim 39 wherein the access controlling code segment causes the computer to reroute the access requestor.

56. (Canceled).

57. (Previously presented) The computer program of claim 39 wherein the access controlling code segment causes the computer to deny subsequent access by the access requestor to the access provider when a number of payload portions that include the predetermined pattern exceed a configurable threshold number during a configurable period of time.

58. (Previously presented) The method as in claim 1 wherein denying communication of subsequent data packets from the access requestor to the access provider further comprises denying communication of subsequent data packets from a group of access requestors to the access provider when a number of payload portions within the data packets that are received, from the access provider by at least one access requester which is a group member, include the predetermined pattern exceed a configurable threshold number.

59. (Previously presented) The method of claim 1 further comprises determining whether the access requestor is on a permitted access list that is associated with the access requestors allowing subsequent access from the access requestor to the access provider conditioned on whether or not the access requestor is determined to be included in the permitted access list.

60. (Previously presented) The method of claim 59 wherein determining whether the access requestor is included in the permitted access list further comprises determining whether the IP address of the access requestor is included in the permitted access list.

61. (Previously presented) The method of claim 1 wherein subsequent data packets from the access requestor to the access provider is denied for a pre-determined and limited period of time.

62. (Previously presented) The method of claim 61 wherein denial of subsequent data packets from by the access provider starts a new pre-determined and limited time period upon detecting an access request the access requestor during the elapsing of the predetermined and limited period of time.

63. (Canceled).

64. (Previously presented) The method of claim 1 wherein denying subsequent data packets from the access requestor is performed in response to a command received from the access provider, irrespective of the inspection of data packets received from the access provider.

65-66. (Canceled).

67. (Previously presented) The method of claim 11 wherein the predetermined pattern further includes a login request message.

68. (Previously presented) The method of claim 11 wherein the login failure message includes a signature located at a specific offset from an end of the data packet communicated from the access provider to the access requestor.

69. (Previously presented) The method of claim 11 wherein the login failure message includes login failure reasons.

70. (Previously presented) The method of claim 1 wherein the network device is a physically independent processor from the access providers.

71. (Previously presented) The method of claim 1 wherein the network device is a switch.

72. (Previously presented) The method of claim 1 wherein the access provider is a device configurable to make a determination of whether access is permitted.

73. (Previously presented) The method of claim 72 wherein the access provider is the field arbitrator of whether access is provided.

Applicant : Brian Jacoby et al.  
Serial No. : 09/894,918  
Filed : June 29, 2001  
Page : 17 of 18

Attorney's Docket No.: 06975-203001 / Security 14

### **Evidence Appendix**

None.

Applicant : Brian Jacoby et al.  
Serial No. : 09/894,918  
Filed : June 29, 2001  
Page : 18 of 18

Attorney's Docket No.: 06975-203001 / Security 14

### **Related Proceedings Appendix**

None.